the nominations, and any statements related to the nominations be printed in the RECORD; that the President be immediately notified of the Senate's action and the Senate then resume legislative session; further, that following this vote, the Senate resume consideration of the EDA bill and vote on the motion to invoke cloture on that bill; that if cloture is not invoked, the Senate proceed to vote to invoke cloture on the motion to proceed to S. 679, the Presidential Appointment Efficiency and Streamlining Act; finally, that the mandatory quorum under rule XXII be waived on both cloture motions.

The PRESIDING OFFICER. Without objection, it is so ordered.

MORNING BUSINESS

Mr. REID. Mr. President, I ask unanimous consent that we now proceed to a period of morning business, with Senators allowed to speak for up to 10 minutes each.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from Rhode Island.

Mr. WHITEHOUSE. Mr. President, I ask unanimous consent that I be allowed to speak for up to 17 minutes.

The PRESIDING OFFICER. Without objection, it is so ordered.

CYBERSECURITY

Mr. WHITEHOUSE. Mr. President, I rise today to speak about a serious issue that touches on our national security, our economic well-being, the safety of our families, and our privacy; that is, America's cybersecurity.

I look forward to conducting an in-depth examination of the aspects of this issue that falls within the Senate Judiciary Committee's jurisdiction during the Subcommittee on Crime and Terrorism's June 21, 2011, hearing, ''Cybersecurity: Evaluating the Administration's Proposals.'' However, because of the importance of improving our cybersecurity, as demonstrated by the recent Gmail spear-fishing attacks and hacks at Sony, Epsilon, Lockheed Martin, and even the Senate itself, I rise to make some initial remarks today.

American technological innovation ushered in the Internet age, bringing with it Facebook, YouTube, and the rest of the World Wide Web. It set off an explosion of new commerce, freedom of expression, and economic opportunity even in the smallest details of our lives—allowing a car company, for instance, to unlock your car doors remotely if you have locked yourself out of your car.

However, this increased connectivity allows criminals, terrorists, and hostile nations to exploit cyberspace, to attack America, to invade our privacy, to loot our intellectual property, and to expose America's core critical infrastructure to cyber sabotage. Entire online communities are dedicated to stealing and selling American credit card numbers. Consider the disturbing fact that the price of your credit card number stolen online actually goes up if the criminal also is selling your mother's maiden name. Some criminals have learned how to spy on Americans, hacking into our home computers and looking out through the video camera attached to the screen. Others run Web sites selling stolen entertainment without paying the American companies that created it. And millions of American computers—millions of American computers—have been compromised by malware slaved to botnets that can record your every keystroke and send it instantaneously across the world to a criminal's laptop.

I firmly believe that cyber crime has put our country on the losing end of the largest illicit transfer of wealth in world history. Whether by copying source code, by industrial espionage of military product designs, by identity theft, by online piracy, or by outright old-fashioned stealing from banks—just doing it the electronic way—cyber crime cripples American innovation, kills jobs here at home, and undermines our economic and national security.

Congress must act to protect Americans from these Internet dangers and to protect our civil liberties. Let me say at the outset that the government must not be allowed to snoop indiscriminately into our online activity, to read our e-mail, or to watch us online. There simply is no need for such an invasion of privacy, and we must move forward with that firmly in mind.

The majority leader has introduced a leadership bill that will be a vehicle for our work. The Commerce Committee, led by Chairman ROCKEFELLER and Ranking Member SNOWE, both of whom I had the privilege to serve with on the Intelligence Committee, and the Homeland Security Committee, led by Chairman LIEBERMAN and Ranking Member COLLINS, reported key bills last year. Chairman LEAHY and the Judiciary Committee have reported important legislation on data breach and other issues central to cybersecurity. The Armed Services, Energy, and other committees have studied the issue from the perspective of their particular jurisdictions and expertise, and under the leadership of Chairman FEINSTEIN, the Intelligence Committee Cybersecurity Task Force completed its classified report last July, authored by me, Senator MIKULSKI, and Senator SNOWE. So we have been ready in Congress.

The administration has now weighed in with its own proposal, recognizing that we need cybersecurity legislation to make our Nation safer and launching in earnest our legislative process.

We have hard work ahead to find the best possible solutions to this complex and grave challenge to our national and economic security. As we begin, I would like to flag five issues that I believe must be addressed as this legislation goes forward.

First, we need to build greater public awareness of cybersecurity threats going forward.

What is the problem? The problem is that information affecting the dot.gov and the dot.mil domains—the government domains—is largely classified. And in the dot.com, dot.net, and dot.org domains, threat information is often kept proprietary by the victim business so as not to worry shareholders, customers, and regulators, or give ammunition to competitors. The result is that Americans are left in the dark about the level of danger that is actually out there on the Internet.

The administration's proposal would require covered businesses to notify customers if their personal information is stolen, expand reporting of cybersecurity threats, and require some public assessments of cyber readiness.

I believe more can still be done on these fronts. I have had the pleasure of working with Senator KYL to introduce S. 931, the Cyber Security Public Awareness Act. I would like to urge interested colleagues to review it and consider including it as part of our larger cybersecurity legislation. That is first.

Second, the Senate needs to ensure that we give private industry the tools necessary for self-defense against cyber attacks.

Proper sharing among and within industries of cybersecurity threat information is vital. The administration took an important step by recommending, subject to various safeguards, enhanced sharing of cybersecurity threat information by the government with private industry. But we may also need to remove legal impediments that unnecessarily limit the sharing of threat information within industries, and we should be prepared to listen here to the private sector's needs as they set up those areas for safe communications about the cyber threats they share.

Third, our Nation does not have basic rules of the road for end users, ISPs, and software and hardware suppliers.

The administration proposal includes important provisions that would move us in the right direction. Assuming that ISPs—Verizon and Comcast and the companies that are actually providing the service—assuming that these companies qualify as critical infrastructure, which is an assumption we should clarify before getting too far down this path, the administration's proposal would require them to develop a standardized framework to address cybersecurity.

Sensible laws and regulations have made our highways safe, and we need similarly to make our information highways safe. Federal procurement can encourage effective cybersecurity standards with appropriate supply chain security so as to improve cybersecurity across the hardware and software industries. These improvements will benefit the government directly, but it will also improve the security of all products on which business and consumers rely.